

JAY EDELSON (Admitted *Pro Hac Vice*)
(jedelson@edelson.com)
RAFEY S. BALABANIAN (Admitted *Pro Hac Vice*)
(rbalabanian@edelson.com)
ARI J. SCHARG (Admitted *Pro Hac Vice*)
(ascharg@edelson.com)
CHRISTOPHER L. DORE (Admitted *Pro Hac Vice*)
(cdore@edelson.com)
EDELSON MCGUIRE, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370

LAURENCE D. KING (SBN 206423)
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, California 94104
Tel: (415) 772-4700

[Additional counsel appear on the signature page.]

Counsel for Plaintiffs and the Putative Class and Subclass

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

IN RE LINKEDIN USER PRIVACY
LITIGATION

Case No. 12-cv-03088-EJD

**PLAINTIFFS' OPPOSITION TO
DEFENDANT'S MOTION TO
DISMISS THE FIRST AMENDED
CONSOLIDATED CLASS ACTION
COMPLAINT**

Date: Feb. 8, 2013
Time: 9:00 a.m.
Judge: Hon. Edward J. Davila
Courtroom: 4 (5th Floor)
Action Filed: June 15, 2012

TABLE OF CONTENTS

1	INTRODUCTION	1
2		
3	FACTUAL BACKGROUND.....	2
4	<i>LinkedIn Promises To Use “Industry Standard Protocols And Technology”</i>	
5	<i>To Protect Customer Information</i>	2
6	<i>Industry Standard Protocols and Technology Require That Companies</i>	
7	<i>Like LinkedIn Protect Their Websites From Common Attacks and</i>	
8	<i>Encrypt User Passwords</i>	3
9	<i>The June 2012 Data Breach Exposes LinkedIn’s Security Failures</i>	4
10	<i>Had Plaintiffs Known That LinkedIn Wasn’t Protecting Their PII, They</i>	
11	<i>Would Not Have Paid As Much For LinkedIn’s Services</i>	5
12	ARGUMENT	5
13	I. PLAINTIFFS HAVE ARTICLE III STANDING BECAUSE LINKEDIN	
14	FAILED TO PROVIDE THEM WITH THE LEVEL OF DATA	
15	PROTECTION THAT THEY BARGAINED AND PAID FOR.....	6
16	A. Plaintiffs Allege Concrete Economic Harm Because They	
17	Overpaid For Their LinkedIn Memberships And Didn’t	
18	Receive The Full Benefit of Their Bargain	6
19	B. Plaintiff Wright Alleges Additional Injury From An Increased	
20	Risk Of Future Harm	10
21	II. LINKEDIN’S STANDING ARGUMENTS AND SUBSTANTIVE	
22	ATTACKS ON THE UCL CLAIM FALL APART	10
23	A. Plaintiffs Have Standing Under The UCL—They Claim That They	
24	Overpaid For LinkedIn’s Premium Service.....	11
25	B. Plaintiffs State Claims Under The UCL for LinkedIn’s	
26	Unfair Conduct	12
27	C. Though Its Unlikely That Any Reliance Requirement Exists, To	
28	The Extent Necessary, Plaintiffs Have Alleged That They Relied	
	On LinkedIn’s Privacy Policy.....	15
	D. Plaintiffs’ UCL Claim Similarly Need Not Be Pled With Particularity	16
	III. PLAINTIFFS STATE CLAIMS FOR BREACH OF CONTRACT	17
	IV. THE BREACH OF IMPLIED CONTRACT AND UNJUST	
	ENRICHMENT CLAIMS ALSO SURVIVE LINKEDIN’S PLEADINGS	
	ATTACKS.....	19

V.	LINKEDIN BREACHED ITS IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING BECAUSE IT CONSCIOUSLY AND DELIBERATELY ACTED IN BAD FAITH	21
VI.	PLAINTIFFS HAVE SUFFICIENTLY STATED CLAIMS FOR NEGLIGENCE AND NEGLIGENCE <i>PER SE</i>	22
	CONCLUSION	24

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES:

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	6
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 554 (2007)	6
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	6, 7, 9
<i>Sierra Club v. Morton</i> , 405 U.S. 727 (1972)	7

UNITED STATES CIRCUIT COURT OF APPEALS CASES:

<i>Bly-Magee v. California</i> , 236 F.3d 1014 (9th Cir. 2001)	17
<i>Chapman v. Pier 1 Imports (U.S.) Inc.</i> , 631 F.3d 939 (9th Cir. 2011).....	7
<i>Chavez v. Blue Sky Natural Beverage Co.</i> , 340 Fed. App'x 359 (9th Cir. 2009).....	7
<i>Davis v. HSBC Bank Nevada, N.A.</i> , 691 F.3d 1152 (9th Cir. 2012).....	15
<i>Doe v. United States</i> , 58 F.3d 494 (9th Cir. 1995)	25
<i>Johnson v. Lucent Tech. Inc.</i> , 653 F.3d 1000 (9th Cir. 2011)	5, 6
<i>Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.</i> , 315 F. App'x 603 (9th Cir. 2008)	23
<i>Kearns v. Ford Motor Co.</i> , 567 F.3d 1120 (9th Cir. 2009)	16, 17
<i>Resnick v. AvMed, Inc.</i> , 693 F.3d 1317 (11th Cir. 2012)	20, 21
<i>Sateriale v. R.J. Reynolds Tobacco Co.</i> , 697 F.3d 777 (9th Cir. 2012).....	16
<i>Schreiber Distrib. Co. v. Serv-Well Furniture Co.</i> , 806 F.2d 1393 (9th Cir. 1986)	25
<i>Shroyer v. New Cingular Wireless Servs., Inc.</i> , 622 F.3d 1035 (9th Cir. 2010).....	13
<i>Vess v. Ciba-Geigy Corp. USA</i> , 317 F.3d 1097 (9th Cir. 2003).....	17

UNITED STATES DISTRICT COURT CASES:

1	<i>Allen v. Hylands, Inc.</i> , 2012 WL 1656750 (C.D. Cal. May 2, 2012)	20
2	<i>Ansanelli v. JP Morgan Chase Bank, N.A.</i> , 2011 WL 1134451 (N.D. Cal. Mar. 28, 2011)	14
3	<i>Astiana v. Ben & Jerry's Homemade, Inc.</i> , 2011 WL 2111796 (N.D. Cal. May 26, 2011).....	20
4	<i>Boysen v. Walgreen Co.</i> , 2012 WL 2953069 (N.D. Cal. July 19, 2012).....	8
5	<i>Claridge v. RockYou, Inc.</i> , 785 F. Supp. 2d 855 (N.D. Cal. 2011).....	10, 23, 24
6	<i>Colucci v. ZonePerfect Nutrition Co.</i> , 2012 WL 6737800 (N.D. Cal. Dec. 28, 2012).....	19, 20
7	<i>Doe I v. AOL, LLC</i> , 719 F. Supp. 2d 1102 (N.D. Cal. 2010).....	9
8	<i>Elias v. Hewlett-Packard Co.</i> , 2012 WL 4857822 (N.D. Cal. Oct. 11, 2012)	16
9	<i>Fraley v. Facebook, Inc.</i> , 830 F. Supp. 2d 785 (N.D. Cal. 2011).....	13
10	<i>In re Apple In-App Purchase Litig.</i> , 855 F. Supp. 2d 1030 (N.D. Cal. 2012)	13
11	<i>In re Ditropan XL Antitrust Litig.</i> , 529 F.Supp.2d 1098 (N.D. Cal. 2007)	15
12	<i>In re Facebook PPC Adver. Litig.</i> , 2010 WL 3341062 (N.D. Cal. Aug. 25, 2010)	14
13	<i>In re Facebook Privacy Litig.</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011).....	9
14	<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012)	11
15	<i>In re Sony Gaming Networks and Customer Data Security Breach Litig.</i> , 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012).....	10, 23
16	<i>In re TFT-LCD (Flat Panel) Antitrust Litig.</i> , 781 F. Supp. 2d 955 (N.D. Cal. 2011).....	18
17	<i>In re Toyota Motor Corp.</i> , 790 F. Supp. 2d 1152 (C.D. Cal. 2011)	7
18	<i>In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Products</i> <i>Liab. Litig.</i> , 754 F. Supp. 2d 1145 (C.D. Cal. 2010)	7
19	<i>Khasin v. Hershey Co.</i> , 2012 WL 5471153 (N.D. Cal. Nov. 9, 2012)	11, 20
20	<i>Kowalsky v. Hewlett-Packard Co.</i> , 2011 WL 3501715 (N.D. Cal. Aug. 10, 2011).....	13
21	<i>Lamke v. Sunstate Equip. Co., LLC</i> , 2004 WL 2125869 (N.D. Cal. Sept. 22, 2004).....	21
22	<i>Larsen v. Trader Joe's Co.</i> , 2012 WL 5458396 (N.D. Cal. June 14, 2012).....	20
23	<i>Low v. LinkedIn Corp.</i> , 2012 WL 2873847 (N.D. Cal. July 12, 2012)	16
24	<i>Olivera v. Am. Home Mortg. Servicing, Inc.</i> , 689 F. Supp. 2d 1218 (N.D. Cal. 2010).....	15
25	<i>Pinel v. Aurora Loan Servs., LLC</i> , 814 F. Supp. 2d 930 (N.D. Cal. 2011)	14
26	<i>Reinhardt v. Gemini Motor Transp.</i> , 2012 WL 2932678 (E.D. Cal. July 18, 2012).....	14, 15
27		

1	<i>Ries v. Arizona Beverages USA LLC</i> , 2012 WL 5975247 (N.D. Cal. Nov. 27, 2012).....	16
2	<i>Rodman v. Safeway, Inc.</i> , 2011 WL 5241113 (N.D. Cal. Nov. 1, 2011).....	18
3	<i>Scripps Health v. Blue Cross & Blue Shield of Kansas, Inc.</i> , 2011 WL 292142 (S.D. Cal. Jan. 26, 2011).....	20
4	<i>Shaterian v. Wells Fargo Bank, N.A.</i> , 2011 WL 5358751 (N.D. Cal. Nov. 7, 2011).....	21
5	<i>Vicuna v. Alexia Foods, Inc.</i> , 2012 WL 1497507 (N.D. Cal. Apr. 27, 2012).....	20
6	<i>Wang v. OCZ Tech. Group, Inc.</i> , 276 F.R.D. 618 (N.D. Cal. 2011)	7
7	<i>Williams v. The Purdue Pharma Co.</i> , 297 F. Supp. 2d 171 (D.D.C. 2003).....	8
8	<i>Woods v. Google, Inc.</i> , 52012 WL 3673319 (N.D. Cal. Aug. 24, 2012)	13
9	STATE COURT CASES:	
10	<i>Applied Equipment Corp. v. Litton Saudi Arabia Ltd.</i> , 7 Cal.4th 503 (1994)	18
11	<i>Biakanja v. Irving</i> , 49 Cal. 2d 647 (1958)	23
12	<i>Careau & Co. v. Security Pacific Business Credit, Inc.</i> , 222 Cal. App. 3d 1371 (1990)	22
13	<i>Klein v. Chevron U.S.A., Inc.</i> , 202 Cal. App. 4th 1342 (2012)	20
14	<i>Kwikset Corp. v. Superior Court</i> , 51 Cal.4th 310 (2011)	11
15	<i>Lewis Jorge Const. Mgmt., Inc. v. Pomona Unified Sch. Dist.</i> , 34 Cal. 4th 960 (2004)	18
16	<i>Rader Co. v. Stone</i> , 178 Cal.App.3d 10 (1986)	19
17	<i>Smith v. Wells Fargo Bank, N.A.</i> , 135 Cal. App. 4th 1463 (2005)	14
18	STATUTES:	
19	Cal. Bus. & Prof. Code § 17200	<i>passim</i>
20	Cal. Bus. & Prof. Code § 22576	14, 24
21	Fed. R. Civ. P. 8.....	19
22	Fed. R. Civ. P. 9(b)	16, 17
23	U.S. Const. art. III.....	<i>passim</i>
24	SECONDARY AUTHORITIES:	
25	24 Williston on Contracts (4th ed. 2002) § 64:1.....	18
26		
27		

INTRODUCTION

This putative class action challenges Defendant LinkedIn Corporation’s (“LinkedIn” or “Defendant”) failure to take even basic steps to safeguard its users’ personal information—a failure that violated its promise to protect “[a]ll information that [customers] provide . . . with industry standard protocols and technology.” (LinkedIn’s Privacy Policy, Dkt. No. 60-2 at 3.) Falling far short of industry norms, LinkedIn instead used outdated security methods that left its users’ information vulnerable to attack. In June 2012, the unthinkable—rather, predictable—happened: hackers exploited LinkedIn’s lax security protocols, gained access to its databases, and stole and published on the Internet millions of customer passwords and other sensitive information.

Plaintiffs Katie Szpyrka (“Szpyrka”) and Khalilah Wright (“Wright”) (collectively “Plaintiffs”) are two of LinkedIn’s paying “premium” customers. Through their First Amended Consolidated Class Action Complaint (“FAC”), Szpyrka and Wright allege that—as made evident by the data breach—LinkedIn failed to provide them with the full services that they bargained and paid for: protection for their information using “industry standard protocols and technology” and that, as a consequence, both overpaid for their premium subscriptions. Plaintiffs allege that LinkedIn’s security lapses breached the express and implied terms of its Privacy Policy, violated California’s Unfair Competition Law (“UCL”) Cal. Bus. & Prof. Code §§ 17200, *et seq.*, and/or negligently caused them damages.

Specifically, and as explained more fully below, LinkedIn’s supposed security measures were antiquated by any industry measure.¹ First, industry standards require that web-based businesses like LinkedIn develop measures to protect their servers from what’s known as “SQL Injection” attacks. LinkedIn didn’t, and as a result, its system was breached. Second, once breached, hackers were able to access and decipher millions of user passwords because LinkedIn failed to encrypt the information using industry standard protocols—LinkedIn used SHA-1, an old and ineffective

¹ Following the filing of these lawsuits LinkedIn has apparently taken steps to modernize its data protection practices. (FAC ¶ 31 (citing An Update On Taking Steps To Protect Our Members, <http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/> (last visited November 26, 2012)).

1 “hashing” process that fell out of accepted use years ago. All told, these defects caused the exposure
2 of the Plaintiff Wrights’ personal information and breached the terms of LinkedIn’s Privacy Policy.

3 In its motion to dismiss, LinkedIn accuses Plaintiffs (really their attorneys) of trying to
4 capitalize on the data breach. This is false. In reality, Plaintiffs seek to hold LinkedIn accountable
5 for its failure to honor its express promise to safeguard their personal information with industry
6 standard data protection practices—basic “protocols and technology”—that would have prevented
7 the data breach in the first instance. Given their informational asymmetry, that the Plaintiffs could
8 not (and did not) realize prior to the data breach that LinkedIn was neglecting its contractual and
9 statutory security duties is to be expected. LinkedIn, and only LinkedIn, has all of the relevant
10 information regarding its supposed data security efforts, which Plaintiffs more than plausibly allege
11 failed to meet industry standards.

12 Its *ad hominem* attacks failing, LinkedIn falls back on two arguments. First, by pretending that
13 its failure to live up to its own Privacy Policy has not caused any injury, LinkedIn asserts that
14 Plaintiffs’ lack standing under Article III or the UCL. According to LinkedIn, only customers who
15 can indisputably prove on the pleadings that they’ve had their identities stolen as a result of a data
16 breach have standing to sue—irrespective of its own failure to protect their data as promised.
17 Second, LinkedIn raises a hodgepodge of issues disputing the elements of Plaintiffs’ UCL and
18 contract claims, the availability of unjust enrichment as a claim under California law, and Plaintiffs’
19 ability to sue for negligence and implied contract claims.

20 As explained below, none of LinkedIn’s assertions have merit. At the very least, Plaintiffs have
21 suffered injury by overpaying for LinkedIn’s services (and thus not receiving the full benefit of
22 their bargain). Likewise, the FAC plainly sets forth the elements of each claim. This Court should
23 deny LinkedIn’s Motion to Dismiss.

24 **FACTUAL BACKGROUND**

25 ***LinkedIn Promises To Use “Industry Standard Protocols And Technology” To Protect Customer*** 26 ***Information.***

27 LinkedIn owns and “operates the world’s largest professional network on the Internet with more

1 than 120 million members in over 200 countries.” (FAC ¶ 12.) Consumers wanting to build or
 2 expand their professional network can register for and purchase a “premium” account with
 3 LinkedIn by visiting its website, www.Linkedin.com. (*Id.* ¶¶ 13, 14, 40, 46.) During the registration
 4 process, consumers are presented with LinkedIn’s User Agreement and Privacy Policy, which
 5 include an express promise by LinkedIn that it will safeguard “[a]ll information that [consumers,
 6 including Plaintiffs and the Class] provide [it] with **industry standard** protocols and technology.”
 7 (*Id.* ¶ 15.) (Emphasis added).

8 ***Industry Standard Protocols and Technology Require That Companies, Like LinkedIn, Protect***
 9 ***Their Websites From Common Attacks and Encrypt User Passwords.***

10 Industry standards require that web-based businesses that promise to secure customer data must
 11 implement certain basic safeguards. First, companies like LinkedIn must protect their websites
 12 against common hacking techniques, including specifically the type of “SQL Injection”² attack that
 13 hackers used to gain access to LinkedIn’s databases in June 2012. (*Id.* ¶¶ 23–25.) Second, industry
 14 standard technology and protocols require companies to adequately encrypt their users’ passwords.
 15 (*Id.* ¶¶ 18–20.) At a bare minimum, companies like LinkedIn must “salt”³ user passwords before
 16 running them through an acceptable hashing⁴ function.⁵ (*Id.* ¶¶ 19, 23, 24.)

17 ² This hacking technique involves exploiting weaknesses existing in a company’s website to
 18 penetrate into back-end databases that contain sensitive user information. (*Id.* ¶ 22.) Oversimplified,
 19 a hacker uses a computer program to automatically add characters to the URL addresses used by the
 20 website to reach an address that permits access to the company’s back-end servers. As the litigation
 21 will demonstrate, industry standards require companies to ward against such attacks by employing
 several defenses, including regular self-testing for SQL vulnerability. Indeed, the Federal Trade
 Commission has filed actions against corporations claiming to secure customer data while
 remaining vulnerable to SQL injection attacks—claiming such representations are unquestionably
 false and constitute unfair or deceptive practices under federal law.² (*Id.* ¶ 24.)

22 ³ “Salting” a password refers to a process whereby random values are combined with a
 23 password before the text is inputted into a function that applies hash marks (“hashing”, described in
 24 the next footnote) to either all or part of the password. (*Id.* ¶ 19.) Thus, and by way of example
 only, to “salt” the password “BREACH”, a program might add the characters “R” “S” “T” and “L”
 so that the password appears as “RBRSEATCLH.”

25 ⁴ “Hashing” refers to a process by which a password is inputted into a cryptographic hash
 26 function and converted into an unreadable, encrypted format. (*Id.* ¶ 18 n.3.) Hence, and again using
 27 the password “BREACH” solely as an example, hashing the “salted” password “RBRSEATCLH”
 could result in an encryption that would appear as “###RSE#T##CL#”.

1 ***The June 2012 Data Breach Exposes LinkedIn's Security Failures.***

2 Sometime in 2012, hackers infiltrated LinkedIn's servers and accessed the database(s)
3 containing its users' sensitive personally identifiable information ("PII"). (*Id.* ¶ 4.) Despite its
4 promise and contractual obligation to use industry standard protocols and technology in storing user
5 data, the data breach revealed that LinkedIn failed to utilize even basic industry standard encryption
6 methods. (*Id.* ¶ 18.) On "a grading scale of A through F, experts say, LinkedIn . . . would get, at
7 best, a 'D' for [its] security." (*Id.* ¶ 20.) Reports indicate that LinkedIn's servers were breached
8 through an "SQL injection" attack, (*Id.* ¶ 22), which *alone* is demonstrative of its failure to meet
9 industry standard security measures. (*Id.* ¶ 23.)

10 Exacerbating the breach is LinkedIn's corresponding failure to encrypt its users' passwords
11 consistent with industry protocols. (*Id.* ¶ 18.) Rather than salt, hash, re-salt and hash, and store them
12 on a separate server, LinkedIn kept its users passwords in an unsalted format using a hashing
13 function known as SHA-1. (*Id.*) This was deficient. First, SHA-1, originally published by the
14 National Security Agency in 1995, is grossly outdated. (*Id.*) Second, as discussed above, storing
15 users' passwords in hashed format without first salting the password offends conventional data
16 security methods. (*Id.*) LinkedIn's failure to implement these industry standard security protocols—
17 as it promised—left users' passwords exposed to any hacker able to bypass LinkedIn's porous outer
18 layer of security. (*Id.* ¶ 21.)

19 On June 6, 2012, hackers publically posted online a list of approximately 6.5 million
20 passwords—including Plaintiff Wright's password—retrieved from LinkedIn's database. (*Id.* ¶¶ 27,
21 49.) Because the passwords were not adequately salted and hashed, individuals were able to quickly
22 decipher a large number of the posted passwords in a matter of hours. (*Id.* ¶ 27.) While it appears
23 that only LinkedIn users' passwords were published, the information taken from LinkedIn's
24

25 ⁵ As the litigation will ultimately show, the industry standard practice is to: (1) salt passwords
26 before inputting them into a hash function, (2) salt the resulting hash value, and (3) then again run
27 the hash value through a hashing function. (*Id.* ¶ 20.) Finally, the fully encrypted password is stored
on a separate and secure server apart from all other user information. (*Id.*)

1 databases was not limited to passwords. (*Id.* ¶ 29.) Instead, on information and belief, hackers also
 2 accessed and stole the other login credentials related to LinkedIn users' e-mail addresses. (*Id.*)

3 ***Had Plaintiffs Known That LinkedIn Wasn't Protecting Their PII, They Would Not Have Paid***
 4 ***As Much For LinkedIn's Services.***

5 During the relevant time period, Plaintiffs were registered LinkedIn premium users. (*Id.* ¶¶ 38,
 6 46.) Plaintiffs were required to pay annual fees (taken in monthly installments) to use LinkedIn's
 7 premium services. (*Id.* ¶¶ 39, 47.) Specifically, Plaintiff Szpyrka paid LinkedIn \$24.95 monthly
 8 from approximately late 2010 to November 2011, and \$26.95 from December 2011 to the present
 9 for LinkedIn's Business level. (*Id.* ¶ 39.) Plaintiff Wright opted for LinkedIn's "Executive" level of
 10 premium services and paid LinkedIn \$99.95 per month. (*Id.* ¶ 47.) When Plaintiffs first registered
 11 their accounts with LinkedIn they agreed to LinkedIn's User Agreement and Privacy Policy. (*Id.* ¶¶
 12 41, 48.) These agreements expressly included the material term that any "[p]ersonal information
 13 you provide will be secured in accordance with industry standard protocols and technology." (*Id.*)
 14 This turned out to be untrue, and, as a result, Plaintiffs overpaid for their premium memberships.
 15 (*Id.* ¶¶ 45, 53.)

16 Following LinkedIn's refusal to even acknowledge its missteps, Plaintiffs bring claims on
 17 behalf of themselves and the Class for: (i) LinkedIn's violation of California's Unfair Competition
 18 Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*), (ii) breach of contract, (iii) restitution/unjust
 19 enrichment (in the alternative to breach of contract), (iv) breach of the implied covenant of good
 20 faith and fair dealing, (v) breach of an implied contract to reasonably safeguard user information,
 21 (vi) negligence, and (vii) negligence *per se*. (*Id.* ¶¶ 62-91, 106-136.) Plaintiff Wright, who alleges
 22 her information was published following the data breach, also brings claims for breach of contract
 23 and restitution/unjust enrichment (in the alternative) on behalf of herself and a Subclass of others
 24 similarly situated whose information was compromised. (*Id.* ¶¶ 92-105.)

25 **ARGUMENT**

26 "On a motion to dismiss, all allegations of material fact are taken as true and construed in the
 27 light most favorable to the nonmoving party." *Johnson v. Lucent Tech. Inc.*, 653 F.3d 1000, 1010

(9th Cir. 2011). While federal pleading standards require more than “formulaic recitation of the elements” of a claim or “naked assertions,” a complaint survives dismissal where it allows the court “to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 554, 555-57 (2007)). Further relevant here in light of LinkedIn’s attacks on the Plaintiffs’ standing, “general factual allegations of injury . . . may suffice to demonstrate standing, for on a motion to dismiss, ‘[the Court] presume[s] that general allegations embrace those specific facts that are necessary to support the claim.’” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). As shown below, the FAC readily satisfies these standards, and LinkedIn’s Motion to Dismiss should be denied.

I. PLAINTIFFS HAVE ARTICLE III STANDING BECAUSE LINKEDIN FAILED TO PROVIDE THEM WITH THE LEVEL OF DATA PROTECTION THAT THEY BARGAINED AND PAID FOR.

LinkedIn’s first argument seizes upon traditional “data breach” cases and asserts that Plaintiffs lack standing to sue under Article III because they don’t allege that the data breach resulted “in any misuse of [their] personal information by a third party.” (Def. Mot. at 9.) This supposed, “no harm no foul” argument misses the point entirely. This is not a case purely about a data breach—rather, this matter arises out of LinkedIn’s failure to honor its promise to protect its customers’ personal information using “industry standard protocols and technology.” The data breach merely exposed LinkedIn’s ongoing failure to honor its commitment to protect their information—Plaintiffs were deprived of the benefit of the bargain when LinkedIn failed to secure it, irrespective of any resultant breach. Thus, the FAC alleges that Plaintiffs suffered harm because they would not have purchased LinkedIn’s service, or would’ve paid substantially less for it, had they known that LinkedIn wouldn’t provide the promised level of security. In addition, the FAC alleges that LinkedIn’s conduct has caused an increased risk of identity theft. These injuries readily satisfy Article III’s standing requirements, as explained below.

A. Plaintiffs Allege Concrete Economic Harm Because They Overpaid For Their LinkedIn Memberships And Didn’t Receive The Full Benefit Of Their Bargain.

Standing requires a plaintiff “demonstrate that [he or she] has suffered a concrete and

1 particularized injury that is either actual or imminent, that the injury is fairly traceable to the
 2 defendant, and that it is likely that a favorable decision will redress that injury.” *Mass v. E.P.A.*, 549
 3 U.S. 497, 517 (2007); *see also Whitmore v. Ark.*, 495 U.S. 149, 154 (1990). At the pleadings stage,
 4 “general factual allegations of injury resulting from the defendant’s conduct may suffice.” *Lujan*,
 5 504 U.S. at 561 (internal citations and quotations are omitted). Relevant here, the “precise dollar
 6 value of [] losses” is not required at the pleading stage, so long as the plaintiff “allege[s] a tangible
 7 loss that can be proved or disproved upon discovery.” *Wang v. OCZ Tech. Group, Inc.*, 276 F.R.D.
 8 618, 625 (N.D. Cal. 2011) (citing *In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales*
 9 *Practices, & Products Liab. Litig.*, 754 F. Supp. 2d 1145, 1166 (C.D. Cal. 2010)).

10 Allegations of concrete economic harm satisfy the injury-in-fact requirement of Article III.
 11 *Chapman v. Pier 1 Imports (U.S.) Inc.*, 631 F.3d 939, 946 (9th Cir. 2011); *see also Sierra Club v.*
 12 *Morton*, 405 U.S. 727, 733 (1972) (“Palpable economic injuries have long been recognized as
 13 sufficient to lay the basis for standing, with or without specific statutory provision for judicial
 14 review.”). Suffering an economic loss confers standing where a plaintiff alleges that he overpaid for
 15 a product or service. *See In re Toyota Motor Corp.*, 790 F. Supp. 2d 1152, 1166 (C.D. Cal. 2011);
 16 *Wang*, 276 F.R.D. at 628 (plaintiff overpaid and suffered economic loss because the defendant’s
 17 “conduct caused him either to buy a product that he would not have bought, or to buy a product that
 18 was inferior, of lower quality and less value, than that offered.”); *In re Toyota Motor Corp.*
 19 *Unintended Acceleration Mktg., Sales Practices, & Products Liab. Litig.*, 754 F. Supp. 2d at 1163
 20 (plaintiff overpaid and suffered economic loss where plaintiffs allege “that he or she would
 21 probably not have purchased or leased his or her Toyota vehicle had the defect been known at the
 22 time of purchase, but certainly would not have paid as much for it”); *Chavez v. Blue Sky Natural*
 23 *Beverage Co.*, 340 Fed. App’x 359, 360–61 (9th Cir. 2009) (finding a sufficient pleading of injury-
 24 in-fact where a plaintiff alleged that he would not have paid for allegedly mislabeled products had
 25 he known the truth about their geographic origins). At the pleadings stage, “general factual
 26 allegations of injury resulting from the defendant’s conduct may suffice.” *Lujan*, 504 U.S. at 561.
 27

Here, Plaintiffs allege that when they created their accounts, they agreed to LinkedIn's User Agreement and Privacy Policy, including the term that "[p]ersonal information you provide will be secured in accordance with industry standard protocols and technology." (FAC ¶¶ 41, 48.) Plaintiff Wright registered for an account in March 2010 and paid approximately \$99.99 per month, and Plaintiff Szpyrka signed up in late 2010 and paid approximately \$24.95 per month for her membership. (*Id.* ¶¶ 38–39, 46–47.) However, as the FAC alleges, LinkedIn did not even come close to providing the level of data protection that it represented, (*Id.* ¶¶ 3, 15, 16, 18, 21, 35, 39, 47), and Plaintiffs allege that they would not have purchased LinkedIn subscriptions (or would have paid substantially less for them) had they known that LinkedIn would not protect their personal information in the manner that it had promised. (*Id.* ¶¶ 43–45, 51–53.) As such, Plaintiffs' plainly allege that they overpaid for their LinkedIn memberships and didn't receive the data security that LinkedIn promised to provide them.

LinkedIn's authorities are inapposite because in those cases the plaintiffs never alleged they would have paid less, or not at all, for the defendants' products had they known of the products' alleged defects. In *Boysen v. Walgreen Co.*, 2012 WL 2953069, at * 6 (N.D. Cal. July 19, 2012), for example, Judge Illston found that the plaintiff failed to show economic harm because he never alleged that the defendant's fruit juice, which allegedly contained amounts of lead and arsenic, failed to perform as advertised or that he would've purchased an alternative juice had the labeling disclosed the presence of such chemicals. This is far different from the instant case where Plaintiffs expressly claim they would've paid less for LinkedIn's services, or not at all, had they known the company's data security strayed so far from industry practices. Likewise, LinkedIn's reliance on *Williams v. The Purdue Pharma Co.*, 297 F. Supp. 2d 171 (D.D.C. 2003), is misplaced. In that case, plaintiffs failed to allege that the product didn't perform as promised in the defendant's advertising. In sharp contrast, Wright and Szpyrka expressly plead that LinkedIn's service (its online social network) failed to perform as LinkedIn represented it would in its Privacy Policy. (FAC ¶¶ 3, 15, 16, 18, 21, 43, 51.)

Should there be any doubt remaining, courts routinely find standing where a defendant charges a customer money for a good or service but fails to honor its own policies in connection with providing the good or service. *See In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011) (“[A] plaintiff who is a *consumer* of certain services (i.e., who ‘paid fees’ for those services) may state [a claim requiring monetary loss] when a company, in violation of its own policies, discloses personal information about its customers to the public.”); *see also Doe I v. AOL, LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010) (same). Here, Plaintiffs allege: (1) that they paid LinkedIn—from \$24.95 to \$99.99 per month—to use its service, (FAC ¶¶ 39, 47), (2) that its Privacy Policy represented that all “[p]ersonal information you provide will be secured in accordance with industry standard protocols and technology[.]” (*Id.* ¶¶ 41, 48), and (3) that LinkedIn violated its Privacy Policy by failing to implement such protections. (*Id.* ¶¶ 3, 15, 16, 18, 21, 35, 39, 47.) As such, Plaintiffs suffered economic harm in the form of overpaying for their LinkedIn memberships and in not receiving the full services for which they contracted and paid—injuries sufficient to confer Article III standing. *See In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 715; *see also Doe I*, 719 F. Supp. 2d at 1111.

Plaintiffs’ injuries are also particular to them, because they affected Szpyrka and Wright personally. *See Lujan*, 504 U.S. at 560 n.1. (“By particularized, we mean that the injury must affect the plaintiff in a personal and individual way.”). Both Plaintiffs agreed to LinkedIn’s Privacy Policy that said the company was going to safeguard their information according to industry standards, both registered for an account, and both paid for LinkedIn’s services. (*Id.* ¶¶ 38–53.) Their particular harm stems from the fact that they both paid monies for data protection services that they never received.

And, the injuries to Plaintiffs are traceable to LinkedIn, which failed to provide the promised level of data protection as evidenced by the data breach. (*Id.* ¶¶ 3, 15, 16, 18, 21, 35, 39, 47.) In the end, there is no question that, based on Plaintiffs’ theory of the case—that they paid for a service that fell short of what was promised—is sufficient to establish standing.

B. Plaintiff Wright Alleges Additional Injury From An Increased Risk Of Future Harm.

In addition to the economic harm established above, LinkedIn's failure to implement contracted and paid-for security protections resulted in the exposure of Plaintiff Wright's personal information—including her password—which was posted on a public website. (FAC ¶ 49.) This alone confers standing on her. *See In re Sony Gaming Networks and Customer Data Security Breach Litig.*, 2012 WL 4849054, at *8–13 (S.D. Cal. Oct. 11, 2012) (finding that the plaintiffs had articulated sufficient particularized and concrete harm to sustain a finding of injury-in-fact where their sensitive personal data, including account information, was exposed during data breach); *see also Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 861 (N.D. Cal. 2011) (allegations that a defendant disclosed personal information alone may confer Article III standing). Thus, the improper dissemination of Wright's personal information increases her risk of future harm, particularly given that her password could potentially be used to access her online accounts with other web-based businesses. (FAC ¶ 28.) Consequently, Wright's allegations of an increased risk of future harm provide an independent basis for standing.

Accordingly, LinkedIn's failure to safeguard the Plaintiffs' personal information is enough to confer standing because it deprived Plaintiffs of the full benefits of their LinkedIn contracts, thereby causing them to overpay for their premium memberships. That potentially only Wright's data was posted on the Internet (along with the passwords of 6.5 million other customers) in no way strips Szpyrka of her ability to seek redress. The Court should therefore readily reject LinkedIn's standing arguments.

II. LINKEDIN'S STANDING ARGUMENTS AND SUBSTANTIVE ATTACKS ON THE UCL CLAIM FALL APART.

LinkedIn also asserts that Plaintiffs lack statutory standing under the UCL. (Def. Mot. at 16–18.) LinkedIn contends that Plaintiffs' loss of their personal information does not constitute “money or property” under the UCL and that Plaintiffs haven't alleged that LinkedIn's data security practices “resulted in any misuse of their personal information.” (*Id.* at 17–18.) These arguments fail for the same reasons discussed above—Plaintiffs plainly allege that they failed to receive what

they contracted for and overpaid as a result. Next, LinkedIn claims it has not acted unfairly and pretends that the UCL allegations are rooted in fraud (which they are not) and cannot stand because Plaintiffs supposedly have not alleged that they read LinkedIn's false representations. As explained below, none of these assertions have merit.

A. Plaintiffs Have Standing Under The UCL—They Claim That They Overpaid For LinkedIn's Premium Service.

To have standing under the UCL, a plaintiff must have "suffered injury in fact and have lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. There are "innumerable ways in which economic injury from unfair competition may be shown." *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 330 (2011). A plaintiff may, for example, (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have, (2) have a present or future property interest diminished, (3) be deprived of money or property to which he or she has a cognizable claim, or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary. *Id.* at 323. "[P]roof of lost money or property will generally satisfy the element of injury in fact." *Id.* at 325. Further, the UCL's injury requirement is satisfied where a plaintiff alleges that he or she bargained to purchase a product or service with certain advertised characteristics but received a product with inferior capabilities and of lower value. *See, e.g., Khasin v. Hershey Co.*, 2012 WL 5471153 (N.D. Cal. Nov. 9, 2012) ("A consumer who relies on a product label and challenges a misrepresentation contained therein can satisfy the standing requirement of section 17204 by alleging . . . that he or she would not have bought the product but for the misrepresentation"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1072 (N.D. Cal. 2012) (UCL standing established where the plaintiff paid an inflated cost for a product as a result of the seller's false statements regarding certain features).

Plaintiffs have UCL standing. The FAC alleges that Plaintiffs relied on LinkedIn's Privacy Policy and would have paid substantially less—or nothing at all—for LinkedIn's premium service had they known that LinkedIn did not (and had no intention to) provide the promised data protection. (FAC ¶¶ 41, 43, 44, 48, 50, 51, 52.) In other words, had LinkedIn accurately represented

1 its data protection measures in its Privacy Policy, Plaintiffs would have refused to purchase the
 2 service (or would have paid less). *See id.* These allegations are sufficient to demonstrate a loss of
 3 “money or property” under the UCL and, contrary to LinkedIn’s argument, have nothing to do with
 4 value of personal information.

5 LinkedIn counters by arguing that the Privacy Policy at issue is the same for both paying and
 6 non-paying customers and, as such, the “bargain that members enter into when upgrading to
 7 premium services is not based on any promise in the Privacy Policy regarding how LinkedIn will
 8 secure data.” (Def. Mot. at 18.) This is not accurate. First, this argument is based on outside facts—
 9 namely, that “members do not agree to any new User Agreement or Privacy Policy when
 10 purchasing upgraded, premium services.” (*Id.*) Second, LinkedIn ignores that many customers—
 11 including Plaintiffs—signed up for a paid subscription at the same time that they initially created a
 12 LinkedIn account. (*See* FAC ¶¶ 38-39, 46-47.) Third, LinkedIn’s theory ignores that the only
 13 sensitive personal information required to create a free account is a person’s email address and
 14 password—paid subscriptions, on the other hand, necessarily require customers to provide LinkedIn
 15 with their full names, telephone numbers, billing addresses, and credit card numbers to pay the
 16 monthly or annual charges. As such, that LinkedIn supposedly offers the same deficient privacy
 17 protections to paying and non-paying members alike simply not relevant—it is reasonable for
 18 LinkedIn’s paying customers to base their decision to upgrade on LinkedIn’s stated data protection
 19 policies before handing over their personal and financial details. Given these facts, LinkedIn’s
 20 failure to provide any support for its assertions is not surprising.

21 As with Article III standing, that Plaintiffs’ overpaid for their LinkedIn memberships is
 22 sufficient to show they lost money or property under the UCL. LinkedIn’s standing arguments thus
 23 fall flat.

24 **B. Plaintiffs State Claims Under The UCL For LinkedIn’s Unfair Conduct.**

25 According to LinkedIn, the UCL claim also fails because Plaintiffs have not alleged that it acted
 26 unfairly. LinkedIn claims that Plaintiffs have only alleged “conclusory statements” to support these
 27

elements. The plain language of the FAC, however, belies this argument.

An “act or practice is unfair if the consumer injury (1) is substantial, (2) is not outweighed by any countervailing benefit to consumers or to competition, and (3) is not an injury the consumers themselves could reasonably have avoided.” *Woods v. Google, Inc.*, 52012 WL 3673319, at *8 (N.D. Cal. Aug. 24, 2012). Ultimately, “‘unfair’ simply means any practice whose harm to the victim outweighs its benefits.” *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1044 (9th Cir. 2010); *see, e.g., Kowalsky v. Hewlett-Packard Co.*, 2011 WL 3501715 (N.D. Cal. Aug. 10, 2011) (finding that the defendant’s conduct was unfair where it made material claims in its advertising and marketing regarding a product, which were false or misleading, or which had no reasonable basis); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 813 (N.D. Cal. 2011) (finding that the defendant’s conduct was unfair where it used the plaintiffs’ information to endorse third-party products and services without consent because the defendant’s conduct has no utility, let alone outweigh the gravity of the alleged harm to the plaintiffs); *In re Apple In-App Purchase Litig.*, 855 F. Supp. 2d 1030, 1041 (N.D. Cal. 2012) (defendant engaged in unfair business practice under the UCL because “Plaintiffs have shown that they suffered substantial harm by incurring charges that they did not explicitly authorize[,] that no benefit existed and Apple does not claim that there was any benefit to consumers or competition.”).

First, Plaintiffs allege that they, as premium customers, suffered a “substantial” injury in the form of overpayments. (FAC ¶¶ 43, 45, 51, 53.) LinkedIn offers nothing to dispute this.

Second, there are no countervailing benefits that flow from LinkedIn’s misrepresentations and its failure to implement the data security technology and protocols that Plaintiffs bargained and paid for. There’s simply no utility to Plaintiffs or the public at-large in misrepresenting the level of data protection that it will provide to customers. And, given the informational asymmetry between LinkedIn and consumers regarding the actual protections it chooses to implement, Plaintiffs could not have reasonably known the truth about LinkedIn’s data protection policies (or lack thereof) or have otherwise avoided the harm caused by LinkedIn’s misrepresentations.

Not surprisingly, courts routinely allow UCL claims premised on “unfair” conduct where the Defendant breaches its own privacy policies. *See In re Facebook PPC Adver. Litig.*, 2010 WL 3341062 (N.D. Cal. Aug. 25, 2010) (“[A] systematic breach of contract may be an unfair business practice.”); *Ansanelli v. JP Morgan Chase Bank, N.A.*, 2011 WL 1134451 (N.D. Cal. Mar. 28, 2011) (“[U]nder California law, ‘a systematic breach of certain types of contracts . . . can constitute an unfair business practice under the UCL.’”); *Smith v. Wells Fargo Bank, N.A.*, 135 Cal. App. 4th 1463, 1483, 38 Cal. Rptr. 3d 653, 672 (2005) (declined to follow on other grounds) (“[I]t appears that a systematic breach of certain types of contracts (e.g., breaches of standard consumer or producer contracts involved in a class action) can constitute an unfair business practice under the UCL.”). Here, Plaintiffs allege that they agreed to and relied on LinkedIn’s User Agreement and Privacy Policy, including the material term that “[p]ersonal information you provide will be secured in accordance with industry standard protocols and technology.” (FAC ¶¶ 41, 48.) As alleged repeatedly, LinkedIn breached its contractual promise to Plaintiffs (and all of its other paying customers) by failing to provide the level of data protection that it represented in its Privacy Policy. (*See id.* ¶¶ 3, 15, 16, 18, 21, 35, 39, 47, 84, 97.) These allegations establish that LinkedIn’s business practices were unfair.

Moreover, the State of California specifically prohibits companies from breaching their own privacy policies. *See* California Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22576 (“COPPA”). Under COPPA, it is unlawful for “an operator of a commercial Web site or online service that collects personally identifiable information” to “fail[] to comply . . . with the provisions of its posted privacy policy.” *Id.* LinkedIn’s privacy policy breaches—specifically its failure to protect “[p]ersonal information . . . with industry standard protocols and technology”—were thus expressly prohibited by California law. (FAC ¶¶ 3, 18, 21, 41, 43, 48, 51.) That LinkedIn violated COPPA further supports a finding of unfairness (or unlawfulness) as “[v]irtually any law, be it federal, state, or local, can serve as a predicate for an action under the UCL.” *See Reinhardt v. Gemini Motor Transp.*, 2012 WL 2932678 (E.D. Cal. July 18, 2012). As such, Plaintiffs’ UCL

claim survives LinkedIn's attacks.⁶

C. Though Its Unlikely That Any Reliance Requirement Exists, To The Extent Necessary, Plaintiffs Have Alleged That They Relied On LinkedIn's Privacy Policy.

To have standing to bring a UCL claim under the unfairness prong, plaintiff need not allege reliance—it is sufficient that the unfair practices caused the injury. *Olivera v. Am. Home Mortg. Servicing, Inc.*, 689 F. Supp. 2d 1218, 1224 (N.D. Cal. 2010) (“For claims based on the “unfair” or “unlawful” prong of the UCL claim, courts have held that the plaintiff need not allege reliance on misrepresentations, and may allege “causation more generally.”) (citing *In re Ditropan XL Antitrust Litig.*, 529 F.Supp.2d 1098, 1105 (N.D. Cal. 2007)). Here, this is plainly satisfied because LinkedIn's failure to provide the agreed-upon security protections caused Plaintiffs to overpay for their premium accounts. But even if reliance was required, Plaintiffs specifically pled that they relied on the Privacy Policy when activating their memberships. (FAC ¶¶ 41, 48.)⁷ LinkedIn, however, says this is not enough. Rather, it insists that Plaintiffs must allege that they specifically saw and “read” the misrepresentation too. (Def. Mot. at 13.) This argument should be rejected for at least two reasons.

First, Plaintiffs allege that the representations contained in LinkedIn's Privacy Policy were an immediate cause for their purchase or subscription to its service—they allege that had they known

⁶ LinkedIn also contends that the UCL claim fails under the alternative test for “unfairness” articulated in *Pinel v. Aurora Loan Servs., LLC*, 814 F. Supp. 2d 930, 940 (N.D. Cal. 2011) (“An unfair business practice under the UCL is ‘one that either offends an established public policy or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.’”) Several courts in this Circuit no longer apply that test to UCL actions brought by consumers. *See Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1170 (9th Cir. 2012). Nonetheless, assuming *arguendo* that the test applies here, Plaintiffs have sufficiently alleged that LinkedIn's business practices were unfair because its conduct was immoral, oppressive, and unscrupulous—it violates a specific California statute—and substantially injurious to consumers where it knowingly (i) failed to protect Plaintiffs' and the Class members' PII with industry standard protocols and technology, which significantly contributed to the hacker's ability to gain access to its network, and to ultimately decipher and disclose Plaintiff Wright's and the Subclass members' PII to the public, and (ii) collected monthly membership fees paid in part for its promise to use industry standard protocols and technology to protect Plaintiffs' and the Class members' PII. (FAC ¶¶ 72–73.)

⁷ Plaintiffs also allege that “had [they] known of Defendant's substandard security procedures and methods of protecting and storing [their] personal information, [they] would have paid less, or not paid at all, for Defendant's services.” (FAC ¶¶ 43, 51.)

1 LinkedIn would leave their personal information exposed, they would not have subscribed to its
 2 premium service (or would have paid less for it). (FAC ¶¶ 41, 43, 44, 48, 50, 51, 52.) Reliance “is
 3 proved by showing that the defendant’s misrepresentations or nondisclosure was ‘an immediate
 4 cause’ of the plaintiff’s injury-producing conduct. A plaintiff may establish that the defendant’s
 5 misrepresentation is an ‘immediate cause’ of the plaintiff’s conduct by showing that in its absence
 6 the plaintiff ‘in all reasonable probability’ would not have engaged in the injury-producing
 7 conduct.” *See Ries v. Arizona Beverages USA LLC*, 2012 WL 5975247 (N.D. Cal. Nov. 27, 2012)
 8 (“So long as the representation that defendants’ products were ‘natural’ was an ‘immediate’ cause
 9 for their purchase, the reliance requirement is met.”). Accordingly, reliance is established.

10 Second, LinkedIn cites no authority requiring a litigant to separately allege that they “read” and
 11 “relied” on a misrepresentation to maintain an unfair practices claim. Rather, LinkedIn’s cases deal
 12 with plaintiffs that failed to allege reliance in the context of fraud claims. *See Sateriale v. R.J.*
 13 *Reynolds Tobacco Co.*, 697 F.3d 777, 793 (9th Cir. 2012) (holding that district court properly
 14 dismissed the UCL claim because plaintiffs did not allege that they relied on any advertisement
 15 when buying cigarettes); *Low v. LinkedIn Corp.*, 2012 WL 2873847 (N.D. Cal. July 12, 2012)
 16 (dismissing false advertising claim because the plaintiffs “never alleged reliance on any specific
 17 representations or advertising....”); *Elias v. Hewlett-Packard Co.*, 2012 WL 4857822 (N.D. Cal.
 18 Oct. 11, 2012) (dismissing UCL fraud claim because the plaintiff did not “allege that Defendants’
 19 alleged misrepresentations influenced his decision to purchase his computer in any way.”).

20 Accordingly, Plaintiffs are not required to plead reliance for their UCL claim made under the
 21 unfairness prong (although they have in any event).

22 **D. Plaintiffs’ UCL Claim Similarly Need Not Be Pled With Particularity.**

23 LinkedIn also argues that Plaintiffs’ UCL claim fails to meet Rule 9(b)’s pleading requirements.
 24 A claim is said to be “grounded in fraud” when a plaintiff alleges “a unified course of fraudulent
 25 conduct and rel[ies] entirely on that course of conduct as the basis of the claim.” *Kearns v. Ford*
 26 *Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). Here, the crux of Plaintiffs’ FAC is that they are
 27

1 suing to recover the monies paid in exchange for a service (i.e., LinkedIn's data protection promise)
 2 that they never received. (FAC ¶¶ 3, 15, 16, 18, 21, 35, 39, 47.) Though they claim LinkedIn's
 3 promise that it would protect their personal information consistent with industry standards was both
 4 incorrect and false, they do not plead a fraud theory. *See Kearns*, 567 F.3d at 1125. Therefore,
 5 Plaintiffs' allegations do not need to meet Rule 9(b) pleading requirements.

6 Nonetheless, even if Plaintiffs' claim was grounded in fraud, the FAC meets Rule 9(b). To
 7 adequately plead claims grounded in fraud, a plaintiff must include particularized allegations that
 8 include the "who, what, when, where and how" of the misconduct charged." *Vess v. Ciba-Geigy*
 9 *Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). Rule 9(b) demands that the circumstances
 10 constituting the alleged fraud "be 'specific enough to give defendants notice of the particular
 11 misconduct . . . so that they can defend against the charge and not just deny that they have done
 12 anything wrong.'" *Bly-Magee v. California*, 236 F.3d 1014, 1019 (9th Cir. 2001).

13 The FAC satisfies these requirements. Plaintiffs allege that when they signed up for their
 14 LinkedIn accounts in March 2010 and late 2010, respectively ("when"), LinkedIn ("who"),
 15 misrepresented in its website Privacy Policy ("where"), that it would protect customer information
 16 by using "industry standard protocols and technology" ("what"), and that Plaintiffs relied on such
 17 misrepresentations and overpaid for their subscriptions ("how"). (FAC ¶¶ 62–77.) Again, Plaintiffs
 18 further allege that had they known that LinkedIn would breach its promise, they would not have
 19 purchased or would have paid less for their memberships. (*Id.* ¶¶ 43, 44, 51, 52.) These allegations
 20 are specific enough to give LinkedIn notice of the particular misconduct so that they can defend
 21 against the charges. *See Bly-Magee*, 236 F.3d at 1019.

22 Accordingly, even if the Court finds that Plaintiffs' claim is grounded in fraud, they have
 23 alleged particularized facts under Rule 9(b).

24 **III. PLAINTIFFS STATE CLAIMS FOR BREACH OF CONTRACT.**

25 As an initial matter, LinkedIn does not dispute that its promise to protect Plaintiffs' PII with
 26 industry standard protocols and technology is a term of the contract. Nor can it. The Privacy Policy
 27

1 is specifically incorporated into the User Agreement presented during activation. (Dkt. No. 60-3, at
 2 2) (“You agree that by registering on LinkedIn . . . you are entering into a legally binding agreement
 3 with LinkedIn . . . based on the terms of [the] LinkedIn User Agreement, and LinkedIn Privacy
 4 Policy, which is hereby incorporated by reference....”). Instead, LinkedIn argues that the breach of
 5 contract claims should be dismissed because the “courts have repeatedly rejected the theory that
 6 loss of personal information alone can form the basis for damages.” (Def. Mot. at 21.) LinkedIn
 7 then contends, without support, that Plaintiffs’ “request for money paid” is actually “a request for
 8 restitution” and that this newly imagined remedy is only available when the contract is
 9 unenforceable. (*Id.* ¶ 22.) LinkedIn’s sleight of hand should be rejected—its arguments plainly
 10 ignore that Plaintiffs’ breach of contract claims seek to recover the amount paid for specific contract
 11 benefits (*i.e.*, an industry acceptable level of data security) that LinkedIn failed to provide.

12 It is hornbook law that damages awarded for breach of contract “seek to approximate the
 13 agreed-upon performance.” *Applied Equipment Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal.4th 503,
 14 515 (1994). The goal is to put the plaintiff “in as good a position as he or she would have occupied”
 15 if the defendant had not breached the contract. 24 Williston on Contracts (4th ed. 2002) § 64:1, p. 7.
 16 Stated differently, “the plaintiff is entitled to damages that are equivalent to the benefit of the
 17 plaintiff’s contractual bargain.” *Lewis Jorge Const. Mgmt., Inc. v. Pomona Unified Sch. Dist.*, 34
 18 Cal. 4th 960, 967-68 (2004); *see, e.g., Rodman v. Safeway, Inc.*, 2011 WL 5241113 (N.D. Cal. Nov.
 19 1, 2011) (denying motion to dismiss plaintiff’s breach of contract claim where plaintiff alleged
 20 overcharges for groceries sold by the defendant through its website); *In re TFT-LCD (Flat Panel)*
 21 *Antitrust Litig.*, 781 F. Supp. 2d 955, 967 (N.D. Cal. 2011) (denying motion to dismiss breach of
 22 contract claim where plaintiff was forced to pay higher prices for a product than they otherwise
 23 would have).

24 Without belaboring the point, Plaintiffs allege a cognizable theory of contract damages here.
 25 Plaintiffs entered into a contract with LinkedIn that specifically stated that LinkedIn would protect
 26 its customers’ personal information by using “industry standard protocols and technology.” (FAC
 27

¶¶ 41, 48.) Plaintiffs paid a monthly fee to LinkedIn in exchange for their memberships, which included the promised data security. (*Id.* ¶¶ 39, 47.) LinkedIn breached the contract by failing to use industry standard protocols and technology to protect Plaintiffs’ and the Class members’ PII as promised. (*Id.* ¶¶ 83, 97.) As such, Plaintiffs were deprived of the bargained-for level of data protection that was required by the contract and they are entitled to recover the portion of their monthly fees that were paid in exchange for such bargain. Discovery, including expert testimony, will ultimately prove the value the promised data security had to members of the putative Class. At this stage, that Plaintiffs pled a classic theory of contract damages—which has nothing to do with either ascribing monetary value to personal information or claims for restitution—defeating LinkedIn’s attacks on the breach of contract claims.

IV. THE BREACH OF IMPLIED CONTRACT AND UNJUST ENRICHMENT CLAIMS ALSO SURVIVE LINKEDIN’S PLEADINGS ATTACK.

LinkedIn contends that the breach of implied contract and unjust enrichment claims should be dismissed because a valid and enforceable contract exists.⁸ (Def. Mot. at 23, 25.) Failing that, LinkedIn argues that unjust enrichment is not a “stand-alone cause of action” under California law and that, in any event, Plaintiffs fail to allege a legal theory that would give rise to a restitutionary remedy. (*Id.* at 25.) These arguments do not withstand scrutiny.

First, LinkedIn ignores that at the pleadings stage, “a plaintiff is permitted to plead inconsistent [] counts.” *See Rader Co. v. Stone*, 178 Cal.App.3d 10, 29 (1986). That is because, “[w]here the exact nature of the facts is in doubt, or where the exact legal nature of plaintiff’s right and defendant’s liability depend on facts not well known to the plaintiff, the pleading may properly set forth alternative theories in varied and inconsistent counts.” *Id.*; *see also* Fed. R. Civ. P. 8(a)(3). Moreover, the unjust enrichment claims were specifically pled in the alternative. *Colucci v. ZonePerfect Nutrition Co.*, 2012 WL 6737800 (N.D. Cal. Dec. 28, 2012) (claims for “unjust

⁸ LinkedIn further contends that the breach of implied contract claim should be dismissed because Plaintiffs have not alleged damages. However, as established in Section III above, Plaintiffs allege a cognizable theory of damages. Therefore, this argument similarly fails.

enrichment may survive the pleadings stage when pled as an alternative avenue of relief.”); *see also* *Scripps Health v. Blue Cross & Blue Shield of Kansas, Inc.*, 2011 WL 292142 (S.D. Cal. Jan. 26, 2011).⁹ Therefore, that Plaintiffs may ultimately prevail on their breach of contract claims doesn’t warrant dismissal of these alternative theories at the pleadings stage (especially where as here, LinkedIn claims to have contract defenses).

Second, and contrary to LinkedIn’s legal survey, unjust enrichment is recognized as independent cause of action in California. Although LinkedIn cites several cases holding that unjust enrichment is not an independent cause of action, LinkedIn ignores recent cases where claims for restitution or unjust enrichment survived the pleadings stage as causes of action. *See Colucci*, 2012 WL 6737800 (“[R]estitution or unjust enrichment may survive the pleading stage....”) (citing *Vicuna v. Alexia Foods, Inc.*, 2012 WL 1497507 (N.D. Cal. Apr. 27, 2012); *Larsen v. Trader Joe’s Co.*, 2012 WL 5458396 (N.D. Cal. June 14, 2012); *Astiana v. Ben & Jerry’s Homemade, Inc.*, 2011 WL 2111796 (N.D. Cal. May 26, 2011)). This Court has similarly allowed such claims. *Khasin*, 2012 WL 5471153, at *9 (“Defendant’s final argument is that Plaintiff’s claim for ‘unjust enrichment’ must be dismissed because California does not recognize ‘unjust enrichment’ as a cause of action. The Court rejects this contention.”). Thus, the unjust enrichment claims should survive dismissal.

Third, Plaintiffs sufficiently allege a legal theory that gives rise to restitution. In the context of data breach cases, where a company fails to properly secure its customers’ data, it cannot “equitably retain their monthly-premiums—part of which were intended to pay for the administrative costs of security. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012). In *AvMed*, plaintiffs filed suit alleging that insurance provider failed to properly implement adequate safeguards to properly protect their electronically-stored personal information. *Id.* In reversing the lower court,

⁹ As with its other authorities, LinkedIn cases are inapposite. Unlike the plaintiffs in *Klein v. Chevron U.S.A., Inc.*, 202 Cal. App. 4th 1342, 1389 (2012) and *Allen v. Hylands, Inc.*, 2012 WL 1656750 (C.D. Cal. May 2, 2012), the Plaintiffs here alleged unjust enrichment *in the alternative to* their breach of contract claims. Moreover, in *Klein*, the court held that a valid and enforceable contract existed between the parties, whereas here, the court has not yet made such a ruling.

the Eleventh Circuit held that plaintiffs sufficiently alleged an unjust enrichment cause of action because the insurance provider did not properly secure its customers' data, and could not "equitably retain their monthly premiums—part of which were intended to pay for the administrative costs of data security...." *Id.* Similarly here, Plaintiffs allege that (i) they conferred a monetary benefit on LinkedIn in the form of fees paid each month, (ii) that LinkedIn "appreciates or has knowledge of such benefit," (iii) that LinkedIn uses the premiums, at least in part, to "pay for the administrative costs of data management and security," and (iv) that LinkedIn "should not be permitted to retain the money belonging to Plaintiffs . . . because Defendant failed to implement the data management and security measures that are mandated by industry standards and by its own privacy policy." (FAC ¶¶ 85–91, 99–105.) Therefore, Plaintiffs sufficiently demonstrated a basis for restitution.¹⁰

V. LINKEDIN BREACHED ITS IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING BECAUSE IT CONSCIOUSLY AND DELIBERATELY ACTED IN BAD FAITH.

LinkedIn argues that the breach of implied covenant of good faith and fair dealing claim should be dismissed because it is duplicative of Plaintiffs' breach of contract claims.¹¹ (Def. Mot. at 26.) LinkedIn is mistaken. A breach of implied covenant of good faith and fair dealing claim is not duplicative of a breach of contract claim where a plaintiff alleges that the defendant intentionally interfered with the Plaintiffs' ability to receive the contract's benefits. *Shaterian v. Wells Fargo Bank, N.A.*, 2011 WL 5358751, at *8 (N.D. Cal. Nov. 7, 2011) ("[T]his rule does not apply where a plaintiff alleges that the defendant acted in bad faith to frustrate the contract's actual benefits."); *see also Lamke v. Sunstate Equip. Co., LLC*, 2004 WL 2125869 (N.D. Cal. Sept. 22, 2004). Here, the basis of Plaintiffs' claims is that LinkedIn acted in bad faith by knowingly failing to safeguard and

¹⁰ At the end of its attack on Plaintiffs' unjust enrichment claims, LinkedIn argues that "any claim for fraud in the inducement must be pled with specificity under Rule 9(b), which Plaintiffs have not done." (Def. Mot. at 26.) Plaintiffs did *not* allege any claim for fraud in the inducement. LinkedIn's argument is therefore not applicable.

¹¹ LinkedIn further contends that the breach of the implied covenant of good faith and fair dealing claim should be dismissed because Plaintiffs have not alleged damages. This argument fails for the reasons explained throughout this brief detailing the Plaintiffs' economic injuries.

1 secure its customers sensitive personal information while intentionally representing publically, in an
2 effort to attract customers, that it would do (and was doing) so. (FAC ¶ 112.)

3 LinkedIn further contends that the claim does not allege “conscious and deliberate” acts.
4 *Careau & Co. v. Security Pacific Business Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990) (a
5 breach must be “prompted not by an honest mistake, bad judgment, or negligence, but rather by a
6 conscious and deliberate act....”). LinkedIn contends that Plaintiffs’ allegation that LinkedIn “acted
7 consciously and deliberately[,]” (FAC ¶ 112), is unsupported by evidence showing that LinkedIn’s
8 failures went beyond “an honest mistake, bad judgment, or negligence.” (Def. Mot. at 27.) This is
9 false. The FAC plainly alleges that LinkedIn *knew* that it was failing to adequately protect the
10 Plaintiffs’ and the Class members’ personal information despite its representations to the contrary.
11 (See FAC ¶¶ 31, 106–113.) (“[T]he passwords publicly posted were, by [LinkedIn’s] own
12 admission, only hashed.”). Therefore, Plaintiffs sufficiently allege that LinkedIn “acted consciously
13 and deliberately,” which will be confirmed through discovery.

14 Accordingly, Plaintiffs’ claim for breach of the implied covenant of good faith and fair dealing
15 claim should not be dismissed.

16 **VI. PLAINTIFFS HAVE SUFFICIENTLY STATED CLAIMS FOR NEGLIGENCE AND** 17 **NEGLIGENCE *PER SE*.**

18 LinkedIn also argues that the negligence and negligence *per se* claims should be dismissed.
19 LinkedIn contends that Plaintiffs have failed to plead any sufficiently cognizable injuries to
20 establish damages, and that, even if they had done so, Plaintiffs’ negligence claims are barred by the
21 economic loss doctrine. (Def. Mot. at 27, 28.) LinkedIn further argues that, in any event, the
22 negligence *per se* claim fails because it’s not an independent cause of action and Plaintiffs failed to
23 adequately plead a statutory violation. (*Id.* at 28, 29.) None of these arguments withstand scrutiny.

24 First, LinkedIn’s assertion that Plaintiffs do not allege damages fails because, as established
25 throughout this response, Plaintiffs allege that they have suffered appreciable, non-speculative harm
26 as a result of LinkedIn’s conduct. (See FAC ¶¶ 33, 49, 53.) Further, Plaintiff Wright alleges that as
27 a result of LinkedIn’s conduct, her and members of the Subclass she represents had their personal

1 information compromised and disclosed to the public. (*Id.* ¶¶ 33, 49, 53.) Such unauthorized and
 2 public disclosure of information, which is alleged to have had some ascertainable value, is
 3 sufficient to allege injury at this stage. *See Claridge*, 785 F. Supp. 2d at 866 (denying defendant’s
 4 motion to dismiss the negligence claim because “plaintiff’s allegations that he was injured by
 5 defendant’s actions in permitting the unauthorized and public disclosure of his PII, which had some
 6 unidentified but ascertainable value, are sufficient to allege an actual injury at this stage.”).

7 Second, LinkedIn’s argument that the economic loss doctrine bars Plaintiffs’ claims ignores that
 8 the rule doesn’t apply where a “special relationship” exists between the parties. *See In re Sony*
 9 *Gaming Networks and Customer Data Security Breach Litig.*, 2012 WL 4849054, at *17 (analyzing
 10 the “special relationship” test where the defendants failed to provide guaranteed data security
 11 measures) (citing *Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.*, 315 F. App’x 603, 605-06
 12 (9th Cir. 2008)). To establish whether a special relationship exists, courts consider (1) the extent to
 13 which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the
 14 plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the
 15 connection between the defendant’s conduct and the injury suffered, (5) the moral blame attached to
 16 the defendant’s conduct, and (6) the policy of preventing future harm. *Kalitta Air*, 315 F. App’x at
 17 605-06. The presence or absence of one factor is not decisive. *In re Sony Gaming Networks and*
 18 *Customer Data Security Breach Litig.*, 2012 WL 4849054, at *10.

19 Each factor is met here. First, the underlying transaction was intended to affect Plaintiffs
 20 because the “end and aim” of the transaction was to provide services to them. (FAC ¶ 122); *see*
 21 *Biakanja v. Irving*, 49 Cal. 2d 647, 650 (1958). Second, the harm to Plaintiffs was foreseeable
 22 because LinkedIn didn’t implement paid-for data security measures and “[d]ata breaches involving
 23 the loss of PII have increased significantly over the past several years.” (*Id.* ¶ 128.) Third, as alleged
 24 in the FAC, (*Id.* ¶ 130), and established throughout this response, Plaintiffs suffered injury as a
 25 result of LinkedIn’s conduct. Fourth, the injury was connected to LinkedIn’s conduct because its
 26 failure to implement paid-for data security measures contributed significantly to the exposure and
 27

1 loss of their PII. (*Id.* ¶¶ 125–26.) Similarly, this supports a finding that the fifth factor—whether
 2 moral blame is attached to LinkedIn’s conduct—is met. (*Id.*) And, sixth, the policy of preventing
 3 future security breaches is substantial. (*Id.* ¶ 128.) Accordingly, the economic loss rule does not bar
 4 Plaintiffs’ negligence claim.¹²

5 Lastly, LinkedIn argues that Plaintiffs’ negligence *per se* claim should fail because it is not an
 6 independent cause of action and because no underlying statutory violation is pled.¹³ Neither
 7 argument prevails. First, courts in this District recognize negligence *per se* as a valid cause of
 8 action. *See Claridge*, 785 F. Supp. 2d at 866. Second, as explained in Section II above, Plaintiffs
 9 have specifically alleged that LinkedIn violated its statutorily imposed standard of care established
 10 by COPPA and the UCL. Therefore, Plaintiffs have stated a valid claim for negligence *per se*.¹⁴

11 CONCLUSION

12 For the foregoing reasons, Plaintiffs Katie Szpyrka and Khalilah Wright, individually and on
 13 behalf of all others similarly situated, respectfully requests that the Court enter an Order (1) denying
 14 LinkedIn’s motion to dismiss in its entirety, (ii) requiring LinkedIn to answer Plaintiffs’ FAC, and
 15 (iii) providing such other and further relief as the Court deems equitable and just.¹⁵

16 ¹² LinkedIn again argues that the “bargain that members enter into when signing up for
 17 premium services is not tied to how LinkedIn secures their data....” (Def. Mot. at 28.) As discussed
 18 in Section II.A above, this argument falls flat—premium customers agree to provide far more
 19 sensitive information. Nevertheless, LinkedIn contends that these allegations fail the “plausibility”
 20 test because Plaintiff Szpyrka (not Wright) remained a premium services member. (*Id.* at 28–29.)
 21 This argument is pure conjecture. Discovery could reveal that Plaintiff Szpyrka chose to remain a
 premium LinkedIn for any number of reasons, including the fact that immediately after the security
 breach, LinkedIn implemented the security measures that it represented it would. (FAC ¶ 31); *see*
 also An Update On Taking Steps To Protect Our Members, [http://blog.linkedin.com/2012/06/09/an-](http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/)
 update-on-taking-steps-to-protect-our-members/ (last visited November 26, 2012).

22 ¹³ LinkedIn further contends that the negligence *per se* claim fails because Plaintiffs did not
 23 allege damages. This argument fails for the same reasons it failed with respect to Plaintiffs’ other
 claims.

24 ¹⁴ Should this Court find that Plaintiffs cannot bring a negligence *per se* claim as an
 25 independent cause of action, Plaintiffs assert that their negligence *per se* claim should survive
 because it is incorporated into Plaintiffs’ negligence cause of action. (FAC ¶¶ 121, 131.)

26 ¹⁵ In the event the Court disagrees with Plaintiffs and grants LinkedIn’s Motion to Dismiss,
 27 Plaintiffs respectfully request leave to add further detail, additional claims, or otherwise take steps

Respectfully submitted,

**KATIE SZPYRKA and KHALILAH
WRIGHT**, individually and on behalf of all
others similarly situated,

Dated: January 22, 2013

By: /s/ Ari J. Scharg
One of Plaintiffs' Attorneys

SEAN P. REIS (SBN 184044)
(sreis@edelson.com)
EDELSON MCGUIRE, LLP
30021 Tomas Street, Suite 300
Rancho Santa Margarita, California 92688
Tel: (949) 459-2124

JAY EDELSON (Admitted *Pro Hac Vice*)*
(jedelson@edelson.com)
RAFEY S. BALABANIAN (Admitted *Pro Hac Vice*)
(rbalabanian@edelson.com)
ARI J. SCHARG (Admitted *Pro Hac Vice*)
(ascharg@edelson.com)
CHRISTOPHER L. DORE (Admitted *Pro Hac Vice*)
(cdore@edelson.com)
EDELSON MCGUIRE, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370

*Interim Lead Counsel for Plaintiffs and the Putative Class and Subclass

LAURENCE D. KING (SBN 206423)**
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: (415) 772-4700

**Liaison Counsel for Plaintiffs and the Putative Class and Subclass

necessary to cure any defects found by the Court in their pleadings. *See Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1401 (9th Cir. 1986); *Doe v. United States*, 58 F.3d 494, 497 (9th Cir. 1995) (leave to amend should be granted even if the plaintiff did not request leave, unless it is clear that the Complaint cannot be cured). LinkedIn's attempt to misconstrue the "numerous" original complaints and the Consolidated Class Action Complaint as previous opportunities to "cure" deficiencies is misplaced. After consolidating the original individual lawsuits into one single action, (Dkt. No. 12), the Court ordered Plaintiffs Szpyrka and Shepherd to file their Consolidated Class Action Complaint. (Dkt. No. 40.) After Plaintiffs Szpyrka and Shepherd filed their Consolidated Class Action Complaint, (Dkt. No. 49), LinkedIn moved to dismiss the Consolidated Class Action Complaint. (Dkt. No. 51.) Plaintiffs thereafter filed the instant FAC, which operates as their first amended operative complaint. Therefore, LinkedIn's argument that Plaintiffs have had numerous opportunities to cure the defects in the FAC is wrong.

Additional Counsel for Plaintiffs and the Putative Class and Subclass:

JOSEPH J. SIPRUT
(jsiprut@siprut.com)
SIPRUT PC
17 North State Street, Suite 1600
Chicago, Illinois 60602
Tel: (312) 236-0000

DAVID C. PARISI
(dcparisi@parisihavens.com)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Tel: (818) 990-1299

DAN MAROVITCH
(dmarovitch@marovitchlaw.com)
MAROVITCH LAW FIRM, LLC
233 South Wacker Drive, 84th Floor
Chicago, Illinois 60606
Tel: (312) 533-1605

CERTIFICATE OF SERVICE

I, Ari J. Scharg, an attorney, certify that on January 22, 2013, I served the above and foregoing ***Plaintiffs' Opposition to Defendant's Motion to Dismiss the First Amended Consolidated Class Action Complaint*** by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Ari J. Scharg_____